BPMN Security Extensions for Healthcare Process

Koh Song Sang, and Bo Zhou
Department of Computer Science,
Liverpool John Moores University,
Liverpool, L3 3AF, UK
S.S.Koh@2014.ljmu.ac.uk, B.Zhou@ljmu.ac.uk

***Abstract*— The modelling of healthcare process is inherently complicated due to its multi-disciplinary character. Business Process Model and Notation (BPMN) has been considered and applied to model and demonstrate the flexibility and variability of the activities that involved in healthcare process. However, with the growing usage of digital information and IoT technology in the healthcare system, the issue of information security and privacy becomes the main concern in term of both store and management of electronic health record (EHR). Therefore, it is very important to capture the security requirements at conceptual level in order to identify the security needs in the first place. BPMN is lacking of the ability to model and present security concepts such as confidentiality, integrity, and availability in a suitable way. This will increase the vulnerability of the system and make the future development of security for the system more difficult. In this paper we provide a solution to model the security concepts in BPMN by extending it with new designed security elements, which can be integrated with the BPMN diagram smoothly.**

***Index Terms* — Security Requirement, BPMN, Healthcare, Internet of Things.**

I. INTRODUCTION

The modern healthcare system is a complex system that combines several of different entities such as institutions, healthcare professionals, patient information, etc. In order to meet the individual needs of different roles, a good understanding of healthcare process is very important. The operation of the system that across inter and intra-organisation interactions needs to be captured and organised at abstraction level. Therefore, a structured modelling language to display the healthcare system concept is urgently needed. Besides, a good healthcare process modelling will also help designing and implementing information system, managing current and future requirements, improving service levels and so on [1]. A general solution to model healthcare process is to apply traditional business process modelling methodologies, although this approach raises several challenges in order to meet the requirements of healthcare system.

There are several standard languages for business process modelling. Business Process Model and Notation (BPMN) is considered the main standard among the others. BPMN was developed by Business Process Modelling Initiative (BPMI) and currently is adopted by Object Management Group (OMG), who provides the standard for businesses in order to present the business processes or procedures by using graphical notations.

The modern healthcare process is getting more participants and organisations involved. It could contain massive communications and interactions between patients, service providers, partners and different departments. Since it is also more common to access healthcare information at remote locations, the information shared between different participants requires better security and access control mechanisms [2]. In fact, the growing usage of digital information such as electronic health record (EHR) brings a lot of convenient to healthcare system but it also raises the security and privacy concerns.

Traditionally, security requirements are only considered after the definition of the business process. However, this inevitably will increase the vulnerability of the system due to the functional behavior of the system and security are normally not independent from each other [4]. It causes the security experts not able to get enough feedback about the system's security requirements. Therefore, security must not be only considered at the technical level, but also at the abstraction level when the business process was defined in the first place. Unfortunately, the notion of security is often neglected in business process models [3] or without being clearly justified. Generally, it is attributed to the fact that business experts do not have enough security-related knowledge or trainings [5]. As a result, the development of security system becomes more difficult afterwards.

Empirical studies show that business experts or end user are actually able to express their security needs at very early stage, thus it is possible to capture and identify their security requirements at the abstraction level as well [3][5]. The problem with that is that currently BPMN does not really support security aspects such as confidentiality, integrity, and availability in a suitable manner [6]. In this paper, we propose a new set of extensions for modelling security concepts in BPMN-based healthcare process. The prototype of these extensions is implemented by enhancing the open source code of a BPMN platform – Activiti.

The rest of the paper is organised as follows. The next section discusses existing work on modelling security concept in BPMN. A new set of extensions with different security requirement are proposed and explained in Section 3. Section 4 presents a case study with the extensions to demonstrate how to model the security requirements in the healthcare process. Finally the paper concludes with an outline of future work in Section 5.

II. RELATED WORK

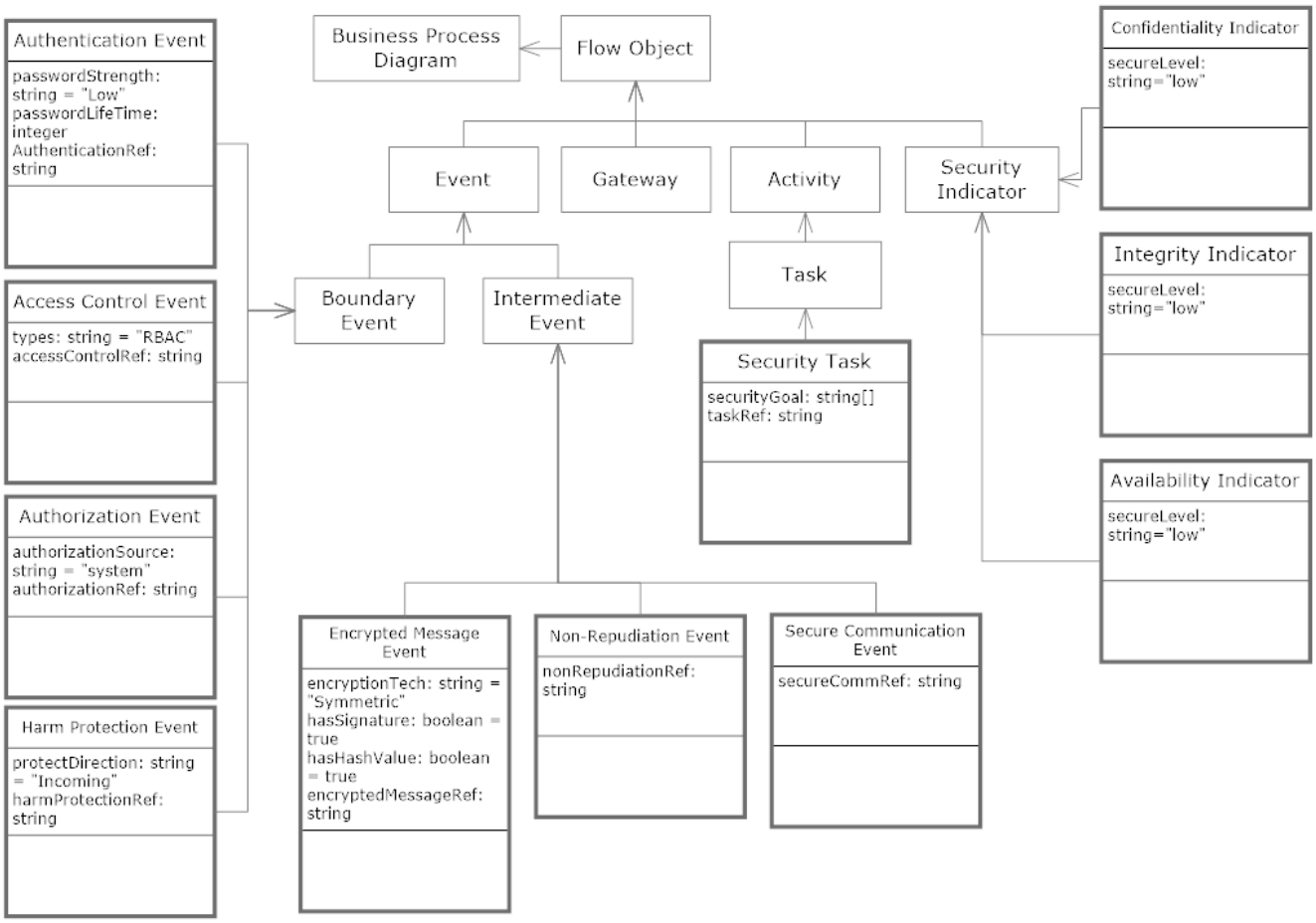

Figure 1 Model view of the security extensions

To the best of our knowledge, modelling the security requirement for healthcare process is still a very fresh topic. However, there are several research papers that are related to analysing security requirements for healthcare system and designing security extensions in BPMN.

According to paper [7], the author outlined a basic security concept in healthcare cloud applications which called "patient-centric" view that widely applied in community healthcare system. Community healthcare system allows the patients to collect, store, use, and share health-related information in a controlled manner with ubiquitous accessibility and offer secure storage and management of patients' electronic health record for several applications. The paper also listed several common security issues for healthcare cloud application which are ownership of information, authenticity, authentication, non-repudiation, patient consent and authorization, integrity and confidentiality of data. Similarly, paper [8] discussed three main information security issues in healthcare system which are information integrity, availability and confidentiality. In this paper we consider these are the ultimate security goals for the healthcare system.

Paper [3] proposed to extend BPMN for security requirement in business processes. It presented five extended Business Process Diagram (BPD) model with the security requirement such as Non-Repudiation, Attack Harm Detection, Integrity, Privacy and Access Control. Each element is represented by a padlock symbol with a corresponding capital letter in the centre and some elements are associated with security role and security permission. However, the extended elements lack the ability to specify response procedures when a security function is failed. This will cause the business expert to neglect the operation of the security processes.

In paper [6], a security language is proposed to be embedded into the BPMN process models as structured text annotations. The author used a Business Process Diagram symbols, namely Artifacts, as a container for constraints. Therefore, security requirements are able to be translated into BPMN model. However, since the security requirement is text-based and hardly understood by business experts, this approach will increase the difficulty to define the security needs.

Besides, paper [4] developed the BPMN extensions with a security language called SecureBPM, which allows for specifying some security requirements such as Access Control, Separation of Duty, Binding of Duty and Need to Know (A subject should only be able to access the information that is strictly necessary for completing a certain task). Furthermore, the author also proposed to apply Model Driven Security (MDS) paradigm to generate Artifacts that allow for generating security configurations for all the services from a single source in order to enforce the security requirements operating at the runtime. Nonetheless, this solution is very limited and lacks considerations for other security requirements such as authentication and non-repudiation.

Table 1 **Extended elements for security sequirements**

Element	Type	Design
Security Task	Task	
Authentication	Boundary Event	
Access Control	Boundary Event	
Authorization	Boundary Event	
Harm Protection	Boundary Event	
Encrypted Message	Intermediate Event	
Non Repudiation	Intermediate Event	
Secure Communication	Intermediate Event	

In summary, some works have been done in the area of both secure healthcare system and BPMN extensions. Yet none of them is comprehensive enough to provide the whole picture of the process and capture the necessary security needs. In the next section we propose a new set of extensions in order to address this issue.

III. SECURITY EXTENSIONS FOR BPMN

In order to capture the security requirements at the abstraction level, we present a set of new designed extensions in BPMN for modelling security concepts in healthcare process. These new extensions, i.e. security notations, are able to work together with the existing BPMN notations and bring several new features to visualize the security requirements in a healthcare system. The extended notations aim at representing the concepts of the security rather than the technology of the security, therefore the technical mechanisms that used to achieve the security requirements are not considered in this case. Instead, it will focus on the specification of the security requirements and how to handle the process if the security function is failed.

Figure 1 presents a model view of the security extensions and shows how these elements are integrated into current BPMN standard. Basically there are three types of element: 1) Security Task is mainly for representing the security-related activities; 2) Security Event is specified for expressing security requirements in healthcare system; 3) Security Indicator is specifically used to indicate the secure level of particular security goals. The security requirements that considered in our solution are Authentication, Authorization, Access Control, Harm Protection, Encrypted Message, Non-Repudiation and Secure Communication. The three security goals that considered in this paper are Confidentiality, Integrity and Availability.

Table 1 lists the design of the new extended notations. From table 1, Security Task and Security Events are inherited from the current BPMN notation design and designed in a standard way with a set of meaningful icons. However, Security Indicators contains brand new designation since it is a new element type of BPMN standard.

For the new extended elements, a security task is a task object that implements general security function in a business process. These security functions could be either handled by human or executed automatically by system. Security Task could be specified at any places exactly like normal BPMN task object. And it is able to attach boundary event and connect to other BPMN elements by using sequence flow or message flow. Typical examples of security task are: running encryption algorithm, physical security lock or data filtering.

A Security Event is an event object that implements specific security function such as Authentication, Access Control in a business process. Unlike Security Task, Security Event enables more specific security requirement than Security Task in the business process modelling. It is able to capture the specific security requirements in a healthcare system and allows security expert to declare the security requirements in a more specific way with its unique attributes. We designed in total seven types of Security Event to represent different security requirements as explained below.

Firstly, Authentication Event is an extended security boundary event that implements the authentication function of the business process modelling. Authentication function is a security process of determining if someone is who he/she declares to be, before granting access to an organisation or system. Authentication Event could be assigned to either Group or Activity of BPMN. When an Authentication Event is specified for a BPMN Activity, it indicates all the processes that these elements contain, have to authenticate the users before they can perform their tasks. Besides, the outgoing sequence flow of Authentication Event determines the process flow when the authentication is failed.

Secondly, an Access Control Event implements the access control function of the business process modelling. Access Control is a security function that controls a selective restriction on access to a particular place or resource from a group of authenticated users. Access Control Event could be assigned to either Group or Activity of BPMN. It indicates the particular processes that are specified inside of these elements must be executed the access control mechanism before executing. The outgoing sequence flow of Access Control Event determines the process flow when the access permission is denied.

Thirdly, an Authorization Event implements the authorization function of the business process modelling. Authorization is a security process that allows an authenticated user who already gained the access permission to a resource to take further actions. Authorization Event could be assigned to either Group or Activity of BPMN. It shows the particular processes attached to these elements must be authorized before executing. The outgoing sequence flow of Authorization Event

determines the process flow when a particular action of a system is unauthorized.

Table 2 Security indicators

Security Indicator	Low	Medium	High
Confidentiality			
Integrity			
Availability			

The forth Security Event is Harm Protection which runs the protection function of the business process modelling. Its functionality is similar to a firewall. Harm Protection establishes a scanning or filtering process in the business process flow in order to protect the system against malicious attacks. It could be specified in any BPMN flow object. A Harm Protection Event indicates the attached process needs to execute its protection mechanism first when the sequence flow arrives. The outgoing sequence flow of Harm Protection Event determines the process flow when an abnormal performance is detected.

Encrypted Message Event is an updated version of the traditional BPMN message event with specifications on encryption. Its functionality is basically the same as the message event. The only difference is that the Encrypted Message Event indicates the content of the message event has either been encrypted or signed in order to protect its confidentiality and integrity.

Furthermore, a Non-Repudiation element indicates the agreement of the interactions between two different roles in order to avoid the denial of the interaction afterwards. It can only be attached to the connection link between two different roles and it does not contain outgoing sequence flow.

Last but not least, a Secure Communication Event indicates the connection between two roles is under certain security protections. Similar to the Non-Repudiation Event, it can only

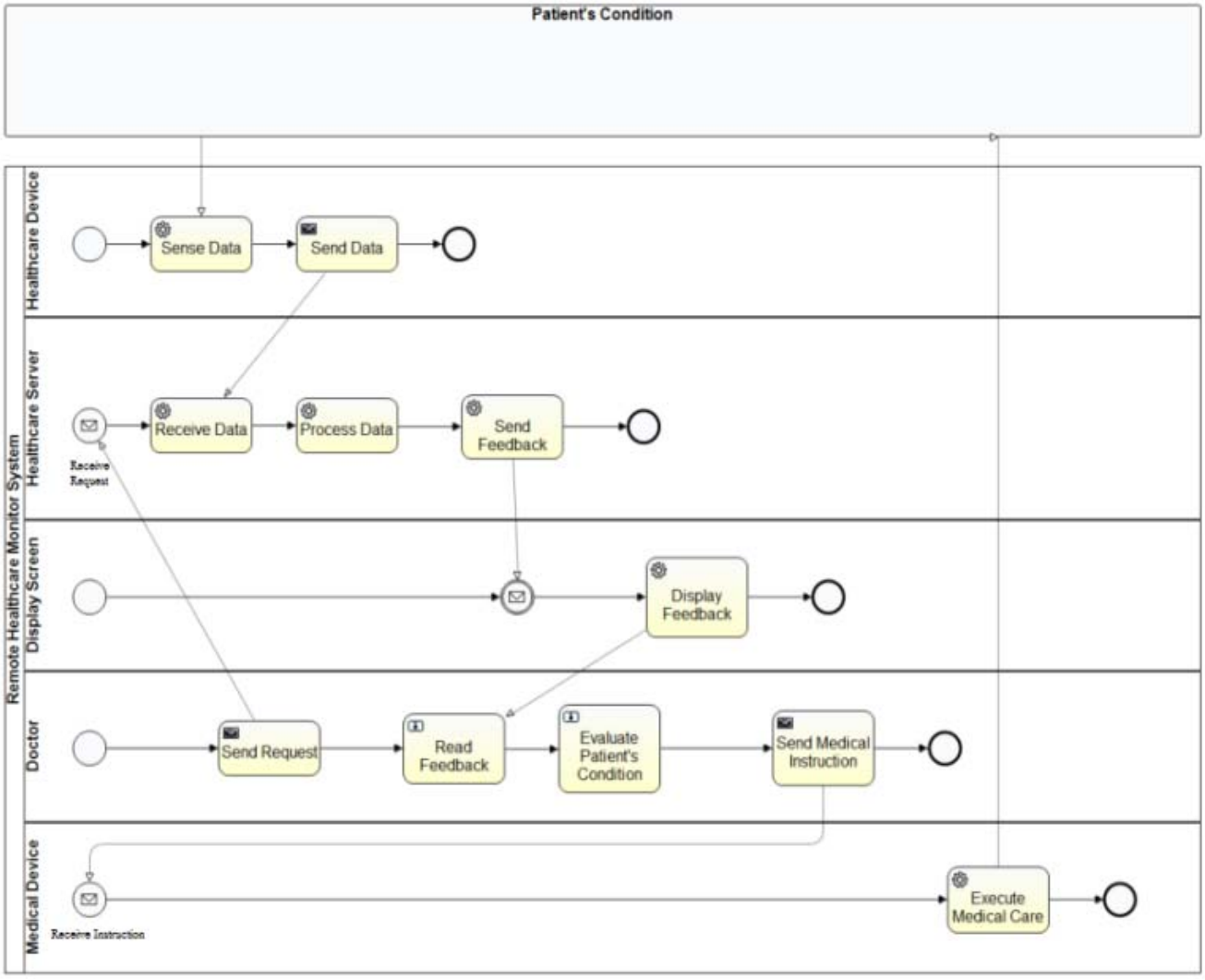

Figure 2 BPMN example of a remote healthcare monitor system

be specified for the connection between roles without outgoing sequence flow.

Finally, the Security Indicator is a new extended element type in BPMN for security purpose. It is designed for indicating the level of security requirement in particular process. The Security Indicator will work together with other process handling element such as the Security Event. Table 2 shows the three Security Indicators used in this paper: confidentiality, integrity, and availability. They serve as a reference of the security strength of a process, and its strength level relies on the security event in the process.

IV. A CASE STUDY

In this section we demonstrate how the Activiti-based BPMN platform is extended and being used to specify security requirements in healthcare process. To achieve this Figure 2 first shows an example BPMN diagram that illustrates a remote healthcare monitor system. It is an IoT-aware BPMN which is composed by five different components. The components are 1) Healthcare Device – a wearable device which is able to sense the patient's body condition, such as blood pressure, heart rate, etc, 2) Healthcare Server – a cloud server that process the patient's body condition data, 3) Display Device – an IoT device for display purpose, 4) Doctor – a medical expert who provides medical services, 5) Medical Device – an IoT device for medical propose.

From the example we can see how the system operates with multiple roles and devices explicitly by using BPMN graphical notations. However, the example could not express the security requirements of the system due to the limitation of current BPMN standard. For instance the Healthcare Server should have executed an authentication function before it processes Doctor's request, and the Medical Device should have checked if the medical instruction is authorized before the execution.

In contrast, in Figure 3 we demonstrate an extended version of the BPMN diagram with the help of our newly designed security elements for representing the security requirements within BPMN. There are several security requirements that are demonstrated here.

A Security Task that executes "Verify Request" is specified

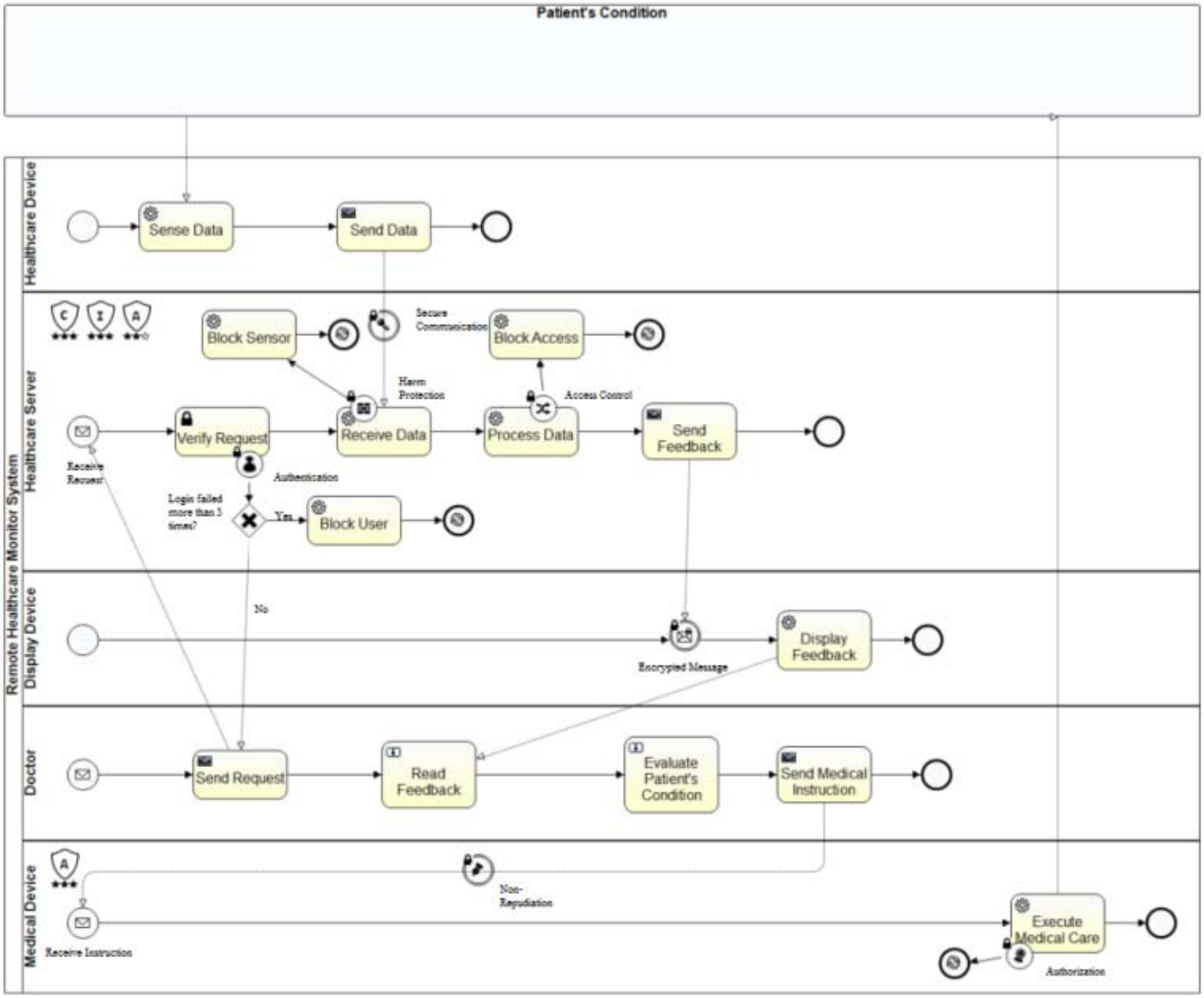

Figure 3 Remote healthcare monitor system with security extensions

after the Healthcare Server receives the request from the Doctor. It indicates that this is a particular task that is actually responsible for a security related task.

An Authentication Security Boundary Event is specified with the "Verify Request" security task. This means the Healthcare Server will run an authentication function before it executes the security task. The outgoing flow of the Authentication event presents the handling process when Authentication is failed. In this case it will block the user if he/she failed to prove his/her identity more than 3 times.

Furthermore, we attached a Harm Protection Security Boundary Event with the "Receive Data" service task. This indicates the Healthcare Server will filter the incoming data from outside in order to protect the system's boundary. If it detects any abnormal performance from the Healthcare device, it will consider the device is compromised and block the device out of the system. Note that there is a Secure Communication Security Intermediate Event is also specified in the middle of the message flow between Healthcare Device and Healthcare Server. It illustrates that the connection between these two components has to be secured.

Moreover, an Access Control Security Boundary Event is drawn after the Healthcare Server receives the data. It is used to make sure the user sending the request does have the access right to the resources. If the user does not have the access right the Healthcare server will block the access and terminate the process with an error message.

When the Healthcare Server sends the feedback to Display Device, an Encrypted Message Security Intermediate Event is specified for the Display Device. This indicates the feedback message that sent from the Healthcare Server is encrypted in order to prevent malicious third party from obtaining the sensitive information.

After the Doctor has read the feedback from the Display Device and examined the patient's condition, he/she will send a medical instruction to the Medical Device to start the medical service. There is a Non-Repudiation Security Intermediate Event that is specified in the middle of the message flow between the Doctor and the Medical Device. This shows that the Doctor cannot deny he/she has sent the medical instruction to the Medical Device and he/she has to be responsible for the instruction.

Finally, there is also an Authorization Security Boundary Event that is associated with the Medical Device which indicates the Medical Device will check whether the Doctor who sends the instruction is authorized to perform this action. If the instruction is unauthorized, the Medical Device will terminate the process with an error message.

In addition to the captured security requirements, this example also illustrates the secure level of different security goals. With the Healthcare Server, three Security Indicators are specified on the top left corner with different protection levels. This indicates that the Healthcare Server needs to have high protection level in Confidentiality and Integrity, and medium protection level in Availability. However, with the Medical Device, it is only required for high protection level in Availability.

As illustrated above, the example shows how our security extensions improve the current BPMN standard in order to support the security requirements specification in the process of modelling Healthcare system. It can be extended to other sectors such as Finance and Transport as well.

V. CONCLUSIONS AND FUTHRE WORK

The security issue in healthcare process is getting more important due to the usage of digital data and cloud-based storage in healthcare process is increasing dramatically. It is crucial to capture the security requirements in a conceptual business process flow in order to reduce the gap of misunderstanding between business expert and security expert. In this paper, we extend the BPMN standard to accommodate security requirements in the first place. It provides the opportunity to improve and raise the security awareness in the healthcare process. A set of security extensions are implemented in Activiti to enable the modelling of the security requirements in healthcare process, which will extensively improve the system's security analysis capability. The usage of the security extensions are illustrated with a simple healthcare example.

For the future work, the next stage of this research will be studying and designing more attributes that related to the specific security requirements to enhance their functionality in BPMN and evaluating the relationship between different security elements and strengthening the interactions among them.

REFERENCES

[1] Amar Ramudhin, Eric Chan, Riadh Benziane, *Abdelkader Mokadem. A New Framework for the Modeling*, *Analysis and Optimization of Pathways in Healthcare.* Service Systems and Service Management, October 2006; p. 698-702.

[2] Ajit Appari, M. Eric Johnson. *Information Security and Privacy in Healthcare: Current State of Research*. August 2008.

[3] Rodriguez A, Fernandez-Medina E, Piattini M. *A BPMN Extension for the Modeling of Security Requirements in Business Processes*. IEICE Transactions on Information and Systems. April 2007. p. 745-752.

[4] Achim D. Brucker, Gero Luckemeyer, Isabelle Hang, Raj Ruparel. *SecureBPMN: Modeling and Enforcing Access Control Requirements in Business Processes.* Proceedings of the 17th ACM symposium on Access Control Models and Technologies. June 2012. p. 123-126.

[5] Yulia Cherdantseva, Jeremy Hilton, Omer Rana. *Towards SecureBPMN - Aligning BPMN with the Information Assurance & Security Domain.* Proceedings of the 4th International Workshop, BPMN 2012, Lecture Notes in Business Information Processing (LNBIP), Springer, p. 107- 115

[6] Jutta Mulle, Silvia von Stackelberg and Klemens Bohm. *A Security Language for BPMN Process Models.* September 2011

[7] Rui Zhang, Ling Liu. *Security Models and Requirements for Healthcare Application Clouds.* Cloud Computing (CLOUD), 2010 IEEE 3rd International Conference on. July 2010. p. 268-275.

[8] Shada Alsalamah, W. Alex Gray , Jeremy Hilton , Hessah Alsalamah. *Information Security Requirements in Patient-Centred Healthcare Support Systems.* 14th World Congress on Medical and Health Informatics. August 2013. p. 812-816.

[9] Object Management Group. *Business process model and notation (BPMN)*, version 2.0, 2011. Available as OMG document formal/2011-01-03.